

**Michigan Supreme Court  
State Court Administrative Office  
309 N. Washington Square, P.O. Box 30048  
Lansing, Michigan 48909  
(517) 373-2222 TEL  
(517) 373-2112 FAX  
Email Ferryj@Jud.state.mi.us  
John D. Ferry, Jr., State Court Administrator**

**M E M O R A N D U M:**

June 13, 2000

TO: Chief Judges  
cc: Court Administrators

FROM: John D. Ferry, Jr., State Court Administrator

RE: SCAO Administrative Memorandum 2000-07  
Trial Court Communications Policies and Procedures

---

With the increased utilization of electronic means of communication, including, but not limited to, telephone and voice mail systems, e-mail (internal), internet e-mail and browsing, facsimile, etc., it has become more important than ever for local trial courts to establish policies and procedures governing internal court use of all communication devices and systems.

Often, these systems are provided through the court's funding unit. In those situations, courts need to establish, **in collaboration with the funding unit**, rules for the control (ownership) and monitoring of data generated by any systems utilized by the court. **Before providing copies of these guidelines to your funding unit, contact your Regional Administrator. He or she can assist you in facilitating the implementation of these policies.**

**A. Control and Monitoring of Court Communications Systems**

**1. Definition**

Communications Systems, include, but are not limited to:

- a. Telephone Systems
- b. Voice Mail
- c. Computer Systems, including internal e-mail
- d. Internet Connections
- e. Facsimile Equipment
- f. Interactive Video

## 2. Policy Requirements

When the court is provided any of its systems through its funding unit, the court should establish procedures, written in collaboration with the funding unit, for the control and monitoring of court information to assure that the information is maintained in a protected and confidential manner. Any question about access to the data and its availability to the public should be covered through these rules.

The rules or controls can be established through three alternatives or combination of alternatives: 1) joint policies and procedures agreed upon with the funding unit (see attached Model Policy for the Operation of Computer Network, Internet Access, E-Mail, Phone Service and Other Communication Equipment and Programs Utilized by the Court); 2) a contract for services between the court and the funding unit; and 3) hardware and software solutions for certain services, such as e-mail and internet access (see Section B: Computer Hardware and Software Options for Judicial E-mail and Internet Autonomy), with necessary internal operating procedures.

No matter which alternative or sets of alternatives are employed, the court should assure that the following provisions are included in any agreement, policy statement, or contract:

All data, information, or records generated in or by any Communications Systems utilized by the judges and employees of the court are the property of the court and shall not be disseminated without written approval of the Chief Judge.

Only the court will have the authority to monitor and review all data, information, or records generated by the judges and employees of the court. The Chief Judge has the sole authority to authorize appropriate action should anyone abuse the use of any system or violate any standard of operation.

The court is encouraged to adopt standards of operation that conform with those adopted by the funding unit so long as those standards do not interfere with the orderly operation of the court. If the funding unit has no standards, the court should adopt standards consistent with recommendations provided by the State Court Administrative Office (see attached Standards for Court Operations of Communication Equipment and Programs).

## B. Computer Hardware and Software Options for Judicial E-Mail and Internet Autonomy

## **1. Introduction**

Courts frequently are users of funding unit data and telecommunications systems. The advantages are obvious. Using the funding unit system offers lower cost of administration due to economy of scale and elimination of redundancy. These arrangements also make it easier to share information locally as needed for the administration of justice.

Sharing information and telecommunications systems does present challenges to the responsibility of courts to independently manage and control information for which the court has legal responsibility to fulfill its case-deciding and administrative duties.

As part of system administration, the funding unit will often impose restrictions and/or monitoring of these services on all departments, including the court. As courts begin to use e-mail as an integral means of communication, confidential correspondence will often reside on the e-mail system.

When making full use of built-in security features, internal e-mail systems are more than 99% secure. Adding internet capability to an e-mail system will reduce that security to approximately 97%. When monitoring functions are used, anyone with "system administrator" access rights will be able to read all mail, including confidential court-related correspondence. "System administrators" who are not judicial employees should not have access to court documents.

## **2. Policy Requirements**

The following configurations provide a range of options to courts when implementing or updating court computer services.

### **a. Court-Only Computer Services**

Courts may choose to acquire their own computer services so they are not reliant on another branch of government for services and security. This option requires adequate funding and access to competent technical support. However, courts often find it difficult to secure funding for their own computer system, especially when the funding unit has reliable, effective computer services available for the court's use.

**b. Segregated Court Network**

Hardware and software products are available that will permit courts to make use of funding unit-provided connectivity while maintaining control of the court computer services. With this option, courts connect to funding unit networks and implement fire walls between the court network and funding unit network. This effectively segregates court-related network traffic from the funding unit network. Courts could then implement their own e-mail gateway server, allowing judicial employees internet e-mail access over the funding unit internet connection, but limiting mail monitoring to court personnel. This option requires less funding and technical expertise than maintaining completely separate systems. Courts choosing this option should conform to existing funding unit software standards in order to minimize integration support problems.

**c. Segregated Virtual Court Server**

A third option is to have the funding unit e-mail server configured with two post offices, one for the court(s) and one for other funding unit departments. The court post office would then be exempted from monitoring. This option requires a high level of trust in that it would be easy for support staff to turn on monitoring of the court post office. A clear, written policy and procedure governing court and funding unit rights and responsibilities is necessary in order to maintain the principle of separation of powers. Separate backup tapes should be run on the two post offices, allowing funding units to refer requests for data to the courts. This option is the most inexpensive option. However, it may not be feasible in all cases, depending on the hardware and software in place.

**C. Standards for Internal Management of Communication Systems**

**1. Introduction**

Standards for internal management of the court's communication systems should ideally be developed for all communication media, i.e. computers, telephones, facsimile machines. The attached standards can be used as a model for internet and e-mail usage, as well as for other communication media. Every court should adopt these standards, or a similar set of standards that conforms to those established by the funding unit, so long as such standards do not interfere with the orderly operation of the court.

For help on implementation of policies and agreements with your funding unit, contact your Regional Administrator. For further technical information, contact Dan Voss at (517)373-2106.

**Model Policy for the Operation of Computer Network, Internet Access,  
E-Mail, Phone Service, and Other Communication Equipment and  
Programs Utilized by the Court**

Purpose:

The purpose of this policy is to provide a framework for the operation of the Court's computer network, Internet access, E-mail, phone service and other communication equipment and programs.

Applicability:

The policy applies to all Court employees, contractors, volunteers and other individuals with access to the Court's systems.

System Ownership:

All data generated by or resulting from the actions of Court employees is the property of the Court. All other data generated by or resulting from the actions of contractors, volunteers and others is also owned by the Court. All requests for information or data generated by the systems must be submitted to the Chief Judge in writing and the Chief Judge will respond to such requests in writing.

Interception of E-Mail, Voice Mail, Telephone Logs, Internet Messages, and Any Other Information Generated Within the System:

The Court reserves the right to monitor and review the contents of information generated by any Court employee as well as any contractors, volunteers or others given access by the Court. The funding unit or its authorized agents will not have the right to monitor, review the contents of nor have access to any information generated by Court employees as well as any contractors, volunteers or others given access by the Court.

Acceptable Standards:

The Court adopts the attached standards for the day to day usage of all communication systems which shall be applicable to all Court employees, contractors, volunteers or others given access by the Court. Violation of any of these standards will subject the individual to appropriate disciplinary action to be determined by the Chief Judge.

Agreement Between Court and Funding Unit

The (insert court name) Court and the (insert funding unit) agree that the Court will advise the funding unit of any violations that could result in liability for the funding unit. In addition, the Court will comply with operational standards adopted by the funding unit for

utilization of systems maintained by the funding unit and not covered by this policy and the standards adopted by the Court so long as such standards do not interfere with the effective and efficient operation of the Court.

Acknowledgment of Policy and Joint Agreement

The Chief Judge of the (insert court name) and (the authorized representative of the funding unit) hereby acknowledge this policy and agree to abide by its terms.

\_\_\_\_\_  
Chief Judge of the (insert court name)

Dated:\_\_\_\_\_

\_\_\_\_\_  
(Funding Unit Representative)

Dated:\_\_\_\_\_

## **Standards for Court Operations of Communication Equipment and Programs**

### **A. Standards for Internet and E-mail Usage**

1. Electronic mail ("E-mail") and use of the Internet to access other computers are two valuable tools that improve the functioning of the court and the efficiency of its employees. Whether E-mail is transmitted internally between court computers or is transmitted to a non-court computer via the Internet, E-mail enhances communication capabilities. Similarly, use of the Internet affords court employees greater access to information, and it increases the ability of court employees to distribute information. All court employees are encouraged to use E-mail and Internet access (if provided) as a fast, efficient, and cost-effective means of communicating and sharing information.
2. Court employees must not misuse E-mail or Internet access. The court provides computers and computer access to its employees so that they can better perform their jobs. E-mail sent by court employees must be of a nature and tone that is consistent with the standard of conduct appropriate to the workplace, and court employees must not solicit or encourage others to send E-mail that fails to meet this standard. Similarly, all other file-sharing and communication across the Internet must meet this same standard of conduct.
3. For purposes of this policy, "E-mail" includes all electronic mail sent or received using court computer equipment, regardless of whether the E-mail is transmitted or delivered by means of a court local network, a court-provided Internet account, or a private Internet account. Likewise, "Internet access" includes all Internet access by means of court computer equipment, regardless of whether the access is through a court-provided Internet account or a private Internet account.
4. The primary allowable uses of E-mail and Internet access are:
  - a. The gathering, exchange, and appropriate dissemination of work-related information, research, analysis, documents, and software.
  - b. Communication and exchange of information for professional development: maintaining an employee's work-related training and education, and discussing issues related to the employee's court activities.
  - c. Activities to further the work of committees and professional societies which the employee has joined in connection with his or her court duties.
  - d. Announcement of new laws; new court decisions; new rules, orders, policies, and bulletins; new services and programs; and any other publicly disseminated court information.

- e. Applying for and administering grants or contracts for Judiciary research and programs.
  - f. Communication committed to E-mail in order to create a permanent record for future use.
  - g. Communications regarding intra-office announcements and activities.
5. Limited personal use of E-mail and Internet access is allowed to the same extent as personal use of office telephones. Such use should be kept to a minimum. Personal use of E-mail and/or the Internet must not interfere with the employee's work and must not result in additional cost to the court.
6. The following uses of E-mail and Internet access are prohibited:
- a. Use for any purpose that violates a law of the United States or a law of the State of Michigan.
  - b. Use for any purpose that violates a Michigan Court Rule, a personnel rule, or a court employment contract.
  - c. Use for any purpose specifically prohibited by the Chief Judge or Court Administrator.
  - d. Use which violates the security, privacy, and confidentiality policies, practices and laws of this court and the State of Michigan including unauthorized release of confidential material.
  - e. Use or access to the intentional display or distribution of files containing the following: obscenity, profanity, pornography; expressions of animosity or bias against individuals, groups or organizations; material in violation of regulations prohibiting sexual harassment or other non-businesslike materials.
  - f. For the intentional display or transmission of sexual images, messages, or cartoons, as well as the use of ethnic slurs, racial epithets or anything that could be construed as harassment, gender bias, race/ethnic bias, or bias against any protected class.
  - g. Use for profit activities (unless specific to the Mission or Vision of the Judiciary or other government agencies).



- h. Use to solicit for commercial ventures or political causes, or for private or personal business transactions, or for partisan or non-partisan political activities, or for political fund raising.
- i. Use for advertising or public relations activities not specifically related to court business.
- j. Use for playing of games or non-business computer activities which generate traffic or consume band widths on any local area network.
- k. Interfering with computers or computing systems, damaging software on other computers, or altering the software on other computers without authorization.
- l. Seeking or obtaining information about files, documents, or other data that are private, confidential, or otherwise not open to public inspection, unless specifically authorized to do so by the file owners; or copying, modifying, or deleting such files, documents, or data without authorization.
- m. Copying or downloading software in violation of copyright or license restrictions, or using evaluation copies of software in violation of license restrictions.
- n. Downloading software without screening it for viruses.
- o. Representing oneself as another without that other person's permission.

**B. Standards for Usage of Telephones, Voice Mail, Facsimile Equipment, Interactive Video and Other Communications Devices**

- 1. The primary allowable uses of telephones, voice mail, facsimile equipment, interactive video and other communications devices are:
  - a. The gathering, exchange, and appropriate dissemination of work-related information, research, analysis, documents, and software.
  - b. Communication and exchange of information for professional development: maintaining an employee's work-related training and education, and discussing issues related to the employee's court activities.
  - c. Activities to further the work of committees and professional societies which the employee has joined in connection with his or her court duties.

- d. Announcement of new laws; new court decisions; new rules, orders, policies, and bulletins; new services and programs; and any other publicly disseminated court information.
  - e. Applying for and administering grants or contracts for Judiciary research and programs.
  - f. Communication committed to a medium which will create a permanent record for future use.
  - g. Communications regarding intra-office announcements and activities.
2. Limited personal use of these media is allowed so long as it does not interfere with the employee's work; does not result in additional cost to the court; is kept to a minimum.
3. The following uses of any communication medium are prohibited:
- a. Use for any purpose that violates a law of the United States or a law of the State of Michigan.
  - b. Use for any purpose that violates a Michigan Court Rule, a personnel rule, or a court employment contract.
  - c. Use for any purpose specifically prohibited by the Chief Judge or Court Administrator.
  - d. Use which violates the security, privacy, and confidentiality policies, practices and laws of this court and the State of Michigan including unauthorized release of confidential material.
  - e. Use or access to the intentional display or distribution of files containing the following: obscenity, profanity, pornography; expressions of animosity or bias against individuals, groups or organizations; material in violation of regulations prohibiting sexual harassment or other non-businesslike materials.
  - f. For the display or transmission of sexual images, messages, or cartoons, as well as the use of ethnic slurs, racial epithets or anything that could be construed as harassment, gender bias, race/ethnic bias, or bias against any protected class.
  - g. Use for profit activities (unless specific to the Mission or Vision of the Judiciary or other government agencies).

- h. Use to solicit for commercial ventures or political causes, or for private or personal business transactions, or for partisan or non-partisan political activities, or for political fund raising.
- i. Use for advertising or public relations activities not specifically related to court business.
- j. Use for playing of games or non-business computer activities which generate traffic or consume band widths on any local area network.
- k. Interfering with computers or computing systems, damaging software on other computers, or altering the software on other computers without authorization.
- l. Seeking or obtaining information about files, documents, or other data that are private, confidential, or otherwise not open to public inspection, unless specifically authorized to do so by the file owners; or copying, modifying, or deleting such files, documents, or data without authorization.
- m. Copying or downloading software in violation of copyright or license restrictions, or using evaluation copies of software in violation of license restrictions.
- n. Downloading software without screening it for viruses.
- o. Representing oneself as another without that other person's permission.